sumo logic

CASE STUDY

暗号資産(仮想通貨)取引所のモニタリング環境を整備 セキュリティと財務諸表監査における IT統制の大幅な強化を実現

bitbank

課題

ビットバンクでは、暗号資産(仮想通貨)取引所のシステムをAWSで運用している。ログのモニタリングにおいては、OSSの分散検索/分析エンジンを利用していたが、アプリケーションの高度なエラー検知や分析などが行えず、セキュリティの確保や財務諸表監査のIT統制の面で不安を抱えていた。

導入経緯

AWSとの親和性の高さや、リソースを柔軟に拡張できることからSumo Logicを採用。大量のデータでも高速で高度な検索が可能となった。非構造化データを自動で構造化する機能や、重要な情報を預ける点において、Sumo LogicはISMSやSOC2、PCIDSSを取得しており、セキュリティ面でも安心できることが採用のポイントになった。トライアル環境で約1カ月間の検証を経て本稼働を遂げた。

導入効果

アプリケーション側で事前にログ収集やログ整形の実装をしなくても、すべてのログをSumo Logicに集約することができた。必要に応じてログの検索や抽出もでき、さらなるセキュリティの強化や財務諸表監査におけるIT統制の対応を実現できた。今後はSumo Logicの権限管理機能を活用し、開発やマーケティングなど全社で高度なログ活用に取り組んでいく。

セキュリティ面での機能不足など ログモニタリングに課題

暗号資産(仮想通貨)取引所「bitbank.cc」を運営するビットバンクは、ビットコインを始めとした仮想通貨の取引量は国内トップレベル*1であり、人気のXRPやモナコインなどの取引量は世界でもトップレベルを誇る。セキュリティについても、第三者機関の調査で日本一を獲得した実績を持つ*2。

同社のシステムはすべてAWS(Amazon Web Services)で構築・運用しているが、ログのモニタリングに課題を抱えていた。

ビットバンク株式会社 セキュリティエキスパート 橋本氏は、「従来は財務諸表監査対応におけるIT統制のためのモニタリングが急務であったため、必要最低限のモニタリングとしてOSSの分散検索/分析エンジンを中心に使っておりましたが、当社サービスのセキュリティ対策を大幅に強化するにあたり、ログモニタリングの範囲を広げたり、複数人でのモニタリング体制整備をしたりする必要がありました。しかし、現在のOSSの分散検索/分析エンジンでは、パフォーマンスやセキュリティ面での機能不足に不安を感じ、モニタリング環境を見直す必要がありました」と振り返る。

さらにビットバンク株式会社 AWSエキスパート 谷津氏は、「ログの分析や活用も十分にできていませんでした。また、その検索/分析エンジンでシステムが複雑化

業種

金融

所在地

東京都品川区西五反田7-20-9
KDX西五反田ビル7F

従業員数

70名

導入ソリューション

Sumo Logic

ビットバンク株式会社
リスク管理部
橋本 健治氏

ビットバンク株式会社
システム部データチーム
チームリーダー
脇本 佑磨氏

ビットバンク株式会社
システム部インフラチーム
谷津 香氏

し、AWSの利用料金もかさんでいました」と続ける。

アプリケーションのエラーのログ検知でも課題が存在していた。ビットバンク株式会社 データ分析エキスパート 脇本氏は、「アプリケーションのエラー検知は、決まったパターンの単純なエラーしか検知できませんでした。通知は上がるものの、詳細は人が判断するなど、効率的ではありませんでした」と明かす。

AWSとの親和性の高さなどから Sumo Logicを採用

ビットバンクでは2019年6月、モニタリング環境の整備に踏み切った。そこで採用されたのが、Sumo Logic社のSaaS型SIEM（Security Information and Event Management）ソリューション「Sumo Logic」である。

選定においては、そのソリューションがクラウド型であり、構築・運用の負荷を軽減できることを重視した。その様子を橋本氏は次のように話す。「Sumo Logicは、当社のシステムと同じAWSで提供されるので、ログの連携が容易で必要に応じてタイムリーにリソースを増減できるなど、多くのメリットがありました」

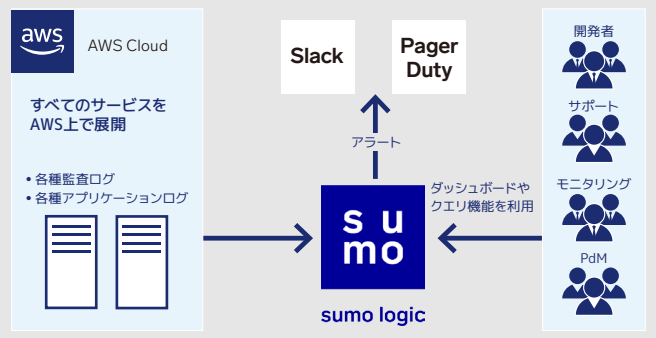
またログデータに関しても、「大量のデータでも検索スピードが速い点を評価しています。非構造化データを自動で構造化データに変換してくれます」と脇本氏は語る。格納するデータ量のみで決まる利用体系や、Sumo Logic自体がISMSやSOC2、PCIDSSなどの国際認定を取得してセキュリティに安心できる点も採用を後押しした。

採用決定後、約1カ月間のトライアル期間を経て、2019年10月に本稼働した。トライアル環境で実データを取り込んで検証し、そのまま本番環境としてリリースした。

「検証用に複数のアカウントを発行してもらえたおかげで、いろいろ試すことができ、効率よく検証を進めることができました」（谷津氏）

ログ収集や検索の効率を大幅に向上 全社でのログ活用も視野に

ビットバンクはSumo Logicの導入によって、充実したモニタリング体制を整備できた。「Sumo Logicのおかげで、財務諸表監査やIT統制対応だけに留まらず、セキュリティ対策の大幅な強化を実現できました。詳細なログ監査の際は高速で高度な検索ができたり、直感的なダッシュボードによって、必要なログをすぐに用意することができたりします」（橋本氏）



さらに運用面において谷津氏は、「高度なログの分析も行えるようになりました。また、従来の検索/分析エンジンを使わなくなったため、システムの複雑化が解消され、そこにかかっていた料金を削減できました」と話す。

アプリケーションのエラー検知についても、「複雑なパターンでの検知が可能となり、サービスの品質をより向上させることができました」と脇本氏は続ける。エラー以外にも、ジョブ実行時間をログから計測し、AWSにかかるコストの最適化に活かすこともできるようになったという。

「従来は収集したいログがあれば、アプリケーション開発の時点で、収集の仕組みを埋め込んでおく必要がありました。Sumo Logicなら、そのような手間をかけなくとも、全体的にログを格納し、後から必要なものを検索することができます。ログ活用の幅が広がり、開発や運用管理の負荷も大きく削減できました」と脇本氏は続ける。

将来的に同社では、不自然に多いログイン動作を検知し、なりすましを事前に防ぐプロアクティブなセキュリティ対策を行うなど、整備したモニタリング環境の活用を加速させていきたいと考えている。

また、システム運用管理のみならず開発やカスタマーサポート、マーケティングなどの担当者にもログ閲覧・分析環境を開放し、業務に活かす構想も考えているという。「Sumo Logicならユーザやログの種類などで権限を細かく設定できるので、セキュリティやコンプライアンスを遵守したまま、全社でログを活用できるでしょう」（橋本氏）

ビットバンクはログ活用を積極的に進めることで、さらなるサービスレベルの向上と競争力の強化に努めていく。

*1 2020年2月20日 CoinMarketCap調べ　*2 2018年10月3日 ICORating調べ

ビットバンクについて

2014年に設立。暗号資産（仮想通貨）取引所「bitbank」を軸に事業展開している。ビットコインをはじめ、6種類の仮想通貨を取り扱う。業界最高レベルに小さいスプレッド（買値と売値の差）、国内ストアでNo.1を取得したことがあるアプリなどで、多くのユーザの支持を集めている。

Sumo Logic ジャパンについて

Sumo Logicは2010年に米国で設立。SaaS型ソリューション「Sumo Logic」は、アプリケーションごとに分散したログを一元管理・分析する。大量のログデータをパターンマッチングで圧縮して人が把握しやすい量にする「LogReduce」、任意の時間、データソースを比較する「LogCompare」など、高度な機械学習分析も提供。ユーザは世界で約2000社にのぼる。2018年10月、日本法人となるSumo Logicジャパン株式会社を設立した。

sumo logic

Sumo Logic ジャパン株式会社
Email: info-jp@sumologic.com

sumologic.jp